Safety in Operations

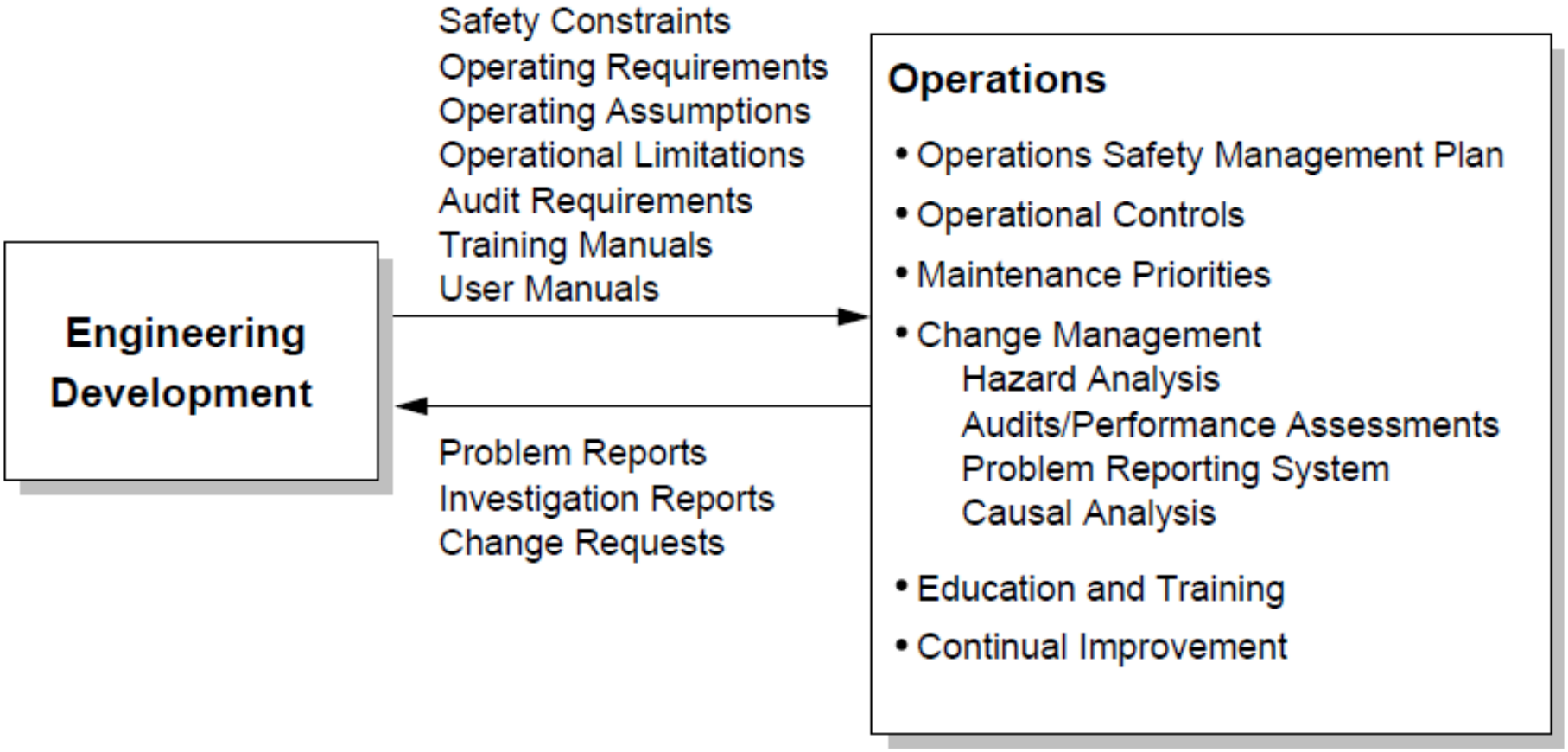
STAMP During Operations

- Goal again is enforcement of safety constraints, this time on operations rather than design
- Pass information that acts as baseline for safe operations
  - Field testing
  - Change analysis
  - Performance audits
  - Incident and accident analysis
- Needs to be specified in way that easy to use during operations

Detecting Development Flaws

- Three goals during operations:
  - Detect safety-related flaws (system design or control structure), hopefully before any accidents
  - Determine why occurred and fix flaws in development
  - Determine whether other flaws may exist
- Want to change culture from a fixing orientation to a learning orientation
- Requires a feedback loop to development

Safety in Operations



Managing/Controlling Change

- Adaptation or change is an inherent part of any system
- Safety control structure must continue to be effective despite changes (including changes in environment, human behavior, organization)
- Controls needed to:
  - Prevent unsafe changes
  - Detect them if they occur

Feedback Channels

- Information flow is key to maintaining safety
- Also need to ensure feedback channels are operating effectively. Cultural problems can interfere with feedback
- Three general types:
  - Audits and performance assessments
  - Reporting systems
  - Accident/incident causal analysis

Audits and Performance Assessments

- Starts from safety constraints and assumptions in safety design
- Need to audit entire safety control structure, not just lower levels
- Audit teams must be free of conflicts of interest
- Participatory and non-punitive audits

Just Culture

Basic Principle: An organization can benefit more by learning from mistakes than by punishing people who make them.

- Reporting errors and suggesting improvements is normal, expected, and without jeopardy.
- Mistake or incident seen not as a failure but a chance to learn
- People are participants in change and improvement
- Information provided in good faith not used against people who report it.

Sidney Dekker, *Just Culture*, 2007

Reporting Systems

- If not being used, then find out why.
- Common reasons why not used:
  - Difficult or awkward to use
  - Information appears to go into a black hole. No point in reporting because organization won't do anything anyway
  - Fear information will be used against them
- Examples of successful systems:
  - Nuclear Power
  - Commercial Aviation

Encouraging Reporting

- Maximize accessibility
  - Reporting forms easily and ubiquitously available
  - Not cumbersome to fill in or send up
- Minimize anxiety
  - Written policy that explains
    - What reporting process looks like
    - Consequences of reporting
    - Rights, privileges, protections, and obligations
  - Without written policy, ambiguity exists and people will disclose less
- Act on reports and send information back (provide feedback)

16.63J / ESD.03J System Safety
Fall 2012